



Frank H. Murkowski, Governor

Edgar Blatchford
Commissioner
PO Box 110800
Juneau, Alaska 99811-0800

NEWS RELEASE

Tina Dickinson
Communications Specialist
907-269-4568
Fax: 907-269-8125
Tina_dickinson@commerce.state.ak.us
www.commerce.state.ak.us

FOR IMMEDIATE RELEASE: November 1, 2004

No. 04-033

CONSUMER ALERT

FDIC Urges Consumers to Be Aware of New Identity Theft Scams

The State Division of Banking and Securities is urging consumers to be more aware of “phishing scams” – as in fishing for confidential information. These are a new types of Internet scams where operators posing as legitimate businesses seek to get consumer information, such as account numbers, passwords, and personal identification numbers (PINS) - leading to both credit card and identity theft.

A common type of phishing scam is where individuals receive e-mails that appear to come from their financial institution. The e-mail may look authentic, right down to the use of the institution's logo and marketing slogans. The e-mails often describe a situation that requires immediate attention, and then warns that the account will be terminated unless the recipient verifies their account information by clicking on a provided link.

The link will take the e-mail recipient to a screen that asks for account information. While it may appear to be a page sponsored by a legitimate financial institution, the information will actually go to the operator who sent the e-mail.

Federal financial regulatory agencies and the State want consumers to know that they should not respond to such requests.

-more-

Consumers should be advised to:

- Never click on the link provided in an e-mail if there is reason to believe it is fraudulent. The link may contain a virus.
- Do not be intimidated by e-mails that warn of dire consequences for not following their instructions.
- If there is a question about whether the e-mail is legitimate, go to the company's site by typing in a site address that you know to be legitimate.
- If you fall victim to a phishing scam, act immediately to protect yourself by alerting your financial institution, placing fraud alerts on your credit files and monitoring your account statements closely.
- Report suspicious e-mails or calls to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

If you suspect that you have been a victim of a phishing scam contact the State Division of Banking and Securities at (907) 465-2521.

For more information on how to avoid these situations go to:

<http://www.fdic.gov/consumers/consumer/news/cnwin0304/phishing.html>

###